

A Revision of a New Chaos-Based Image Encryption System: Weaknesses and Limitations

Hassan Noura*, Lama Sleem[†], Raphaël Couturier[‡]

*Lebanese University, Faculty of Engineering, Department of Computer Science and Telecommunication, Beyrouth, Lebanon

^{†‡}FEMTO-ST Institute, UMR 6174 CNRS - Univ. Bourgogne Franche-Comté (UBFC), Belfort, France

Email: *hnouran@gmail.com, [†]lama.sleem@univ-fcomte.fr, [‡]raphael.couturier@univ-fcomte.fr

Abstract—Lately, multimedia encryption has been the focus of attention in many researches. Recently, a large number of encryption algorithms has been presented to protect image contents. The main objective of modern image encryption schemes is to reduce the computation complexity in order to respond to the real time multimedia and/or limited resources requirements without degrading the high level of security. In fact, most of the recent solutions are based on the chaotic theory. However, the majority of chaotic systems suffers from different limitations and their implementation is difficult at the hardware level because of the non integer operations that are employed requiring huge resources and latency. In this paper, we analyze the new chaos-based image encryption system presented in [1]. It uses a static binary diffusion layer, followed by a key dependent bit-permutation layer that only iterates for one round. Based on their results in this paper, we claim that the uniformity and avalanche effect can be reached from the first round. However, we tried to verify the results but our conclusion was that these results were wrong because it was shown that at least 6 iterations are necessary to ensure the required cryptographic performance such as the plain-sensitivity property. Therefore, the required execution time must be multiplied by 6 and consequently this will increase the latency. In addition to all aforementioned problems, we find that ensuring the avalanche effect in the whole image introduces a high error propagation. In order to solve this problem, we recommend to ensure the avalanche effect in the level of blocks instead of the whole image.

Index Terms—Avalanche effect; Key derivation function; Key-dependent P-box ; Key-dependent integer or binary diffusion matrix; Security analysis.

I. INTRODUCTION

Encrypting images is a necessary requirement to protect the privacy of people and the confidentiality of image contents. However, traditional cryptographic techniques, using symmetric-key standard encryption algorithms such as DES [2] and AES [3], are not efficient for encrypting images and video contents due to the intrinsic features of images, and the strong correlation among the adjacent pixels [4]. Therefore, traditional encryption techniques cannot fit the real-time delivery of multimedia streams according to [5] and discovering another solution becomes absolutely necessary.

Another paradigm has been investigated by researchers in the last decade, which is the "Chaos" field. Chaos consists of a non-linear dynamic system that appears to be random. Due to the extreme sensitivity to initial conditions, chaos was

integrated extensively to build the cryptographic algorithms of digital images such as in [6], [7], [8], [9], [10], [11], [12], [13]. Unfortunately, chaos-based encryption algorithms are not always secure, and most of them have been successfully crypt-analyzed [14], [15], [16], due to their instability coming from the periodicity of mapping [17] and the finite computing precision that renders the system vulnerable to different kinds of attacks [18], [19]. Additionally, the main disadvantage of the majority of chaotic encryption algorithms is the use of **floating calculations** which makes the practical software or hardware implementation of such systems not efficient and complex compared to the traditional ciphers such as AES and DES, which only operate with integer operations.

Recently, a scheme was presented in [1]. It consists in applying a static binary diffusion layer followed by a key dependent bit-permutation based on the periodicity 2D cat map that only iterates for **one round**. In fact, the authors indicated that the avalanche effect can be reached from the first round.

A. Motivation & Contributions

The main motivation of our work is to analyze the previous work of [1] and to quantify its security and performance level to validate whether it can be a good encryption candidate or not.

In this paper, we detail all the weaknesses of this proposal and we prove that the avalanche effect is not attained. In addition, we focus on the weak key size permutation technique and its inflexibility that **limits** the use of this cipher.

However, according to the tests done in this paper, it is shown that the sufficient number of iterations r needed to reach the avalanche effect (plain-sensitivity property) is ≥ 6 . Therefore, the required execution time of this scheme should be multiplied by 6. Based on the obtained results, we demonstrate that [1] does not meet the main contribution needed which is a lower latency. Therefore, we prove that the required latency and resources are so high to ensure the required robustness against attacks. In fact, with $r = 1$, the system is considered weak against different kinds of attacks such as known/chosen plain-text/cipher-text attacks. In addition, it cannot be used by tiny devices such as our smart-phones or sensors because of the high required memory size. More important, we validate that it is extremely sensitive against the channel error thus

preventing its practical implementation. We highlight all these points and give the correct results that should have been taken into consideration.

B. Organization

The rest of this paper is organized as follows. In Section II, an analysis of the proposed scheme of [1] is presented and the weak points are detailed. Moving to Section III, the false result of the avalanche effect is proved in addition to quantify the difference between original and cipher images.. Furthermore, the uniformity analysis is done. Then, in Section IV, the propagation of error analysis shows that any noise affecting the channel will prevent the recovery of the original contents after decryption. The visual degradation analysis was done by studying PSNR [20] and SSIM [21]. Then, a general performance analysis in addition to the execution time is discussed in Section V. Finally, in Section VI, a conclusion summarizes our work and future works are presented.

II. ANALYSIS OF THE PROPOSED CHAOS-BASED IMAGE ENCRYPTION SYSTEM

In this section, we analyze the cipher scheme of [1] that is illustrated in Figure 1. In fact, several points are presented and prove that the proposed cipher cannot reach the efficiency and the required cryptographic performance. As a result, this solution can be seen as unsafe. All details are shown in the following:

- 1) **Low cryptographic performance and attacks vulnerability** : A low number of rounds r based on wrong results enables to reduce the execution time. More important, the security level here is considered low since the plain sensitivity is very low. This makes chosen/known plain-text attacks easy. Additionally, the size of the permutation key used is $4 \times q$, where $q = \lceil \log_2(M) \rceil$ is dependent on the size of the square input image ($M \times M$), which is feasible for any brute force attack and specifically for small sized images. Therefore, this algorithm cannot resist different kinds of attacks. Also, the static structure of the binary diffusion matrix which is independent of the key is not preferable from cryptographic viewpoints and should be dependent on a generated key to strengthen its security level. Also, the dimension of the diffusion matrix is fixed, which removes the flexibility property.

Moreover, in their paper, the authors considered that the permutation was done only once. Therefore, the chaotic generator should be iterated once to produce the required parameters and initial conditions of the permutation technique that has 32 bit length for $M \leq 256$. In fact, this is not sufficient to ensure a sufficient length of permutation sub-key and consequently cannot resist the brute force attacks and is not enough to reach the required cryptographic performance [22] (see chapter 3).

On the other hand, the generator may require to iterate twice for $M \geq 256$ that means that the length of the

required static pseudo-random bits is 64 and it is also not sufficient to break the brute force attacks [22]. In addition to that, as the round of permutation $rp=1$ and the permutation technique is periodic, this means that the produced permutation table has a short period according to [23]. This paper **validates the employment of different parameters and initial conditions for several iterations to prevent the periodicity of permutation.**

- 2) **Not flexible**: The employed permutation technique is based on the Noura formulation of the 2D cat map that was previously presented in [24](see page 90-91). Additionally, the proposition of using invertible binary diffusion matrix for image encryption was also presented previously in [24](see page 113-121) and it is not the original proposition of [1]. Unfortunately, this permutation technique is not flexible and it requires the size of the original image to be square. This is another limitation for this approach since a good approach must be flexible for any dimension desired by the user.
- 3) **High size of memory**: Employing bit permutation instead of byte permutation increases the required memory size by a factor of 8, which is unacceptable for different systems. For example, tiny devices are not able to apply this approach since their memory is limited.
- 4) **Higher latency**: The design of the round function with the goal to reach the avalanche effect with lower round number is not achieved. Moreover, the bit permutation algorithm is realized in the bit level and not in the byte level as in AES. This introduces an overhead in terms of execution time since the operation in byte or word level as in AES is more efficient compared to the bit level as in DES.
- 5) **Difficulty to adapt to modern devices**: Low execution time and low memory requirements are all mandatory conditions to have an efficient cipher that can take into consideration the short life of batteries and the low resources available especially for tiny devices such as sensors or smart phones.
- 6) **High error propagation**: The analysis scheme has a trade-off between the avalanche effect and the propagation error. In fact, the obtained result indicates that a random bit error can destroy the contents of the image, which is not suitable for some applications, especially in wireless communication where the channels are subjected to different kinds of noises [25].

Therefore, all these challenges and weaknesses clearly indicate that the cipher scheme of [1] is neither efficient nor secure and cannot be considered as a good image encryption candidate.

III. ANALYSIS OF THE AVALANCHE EFFECT, SENSITIVITY, AND UNIFORMITY

A. Avalanche effect

Indeed, authors of [1] indicated that the proposed cipher can reach the Avalanche effect after one iteration ($r=1$ see Figure 7 in [1]), which is not true and it was obtained for a

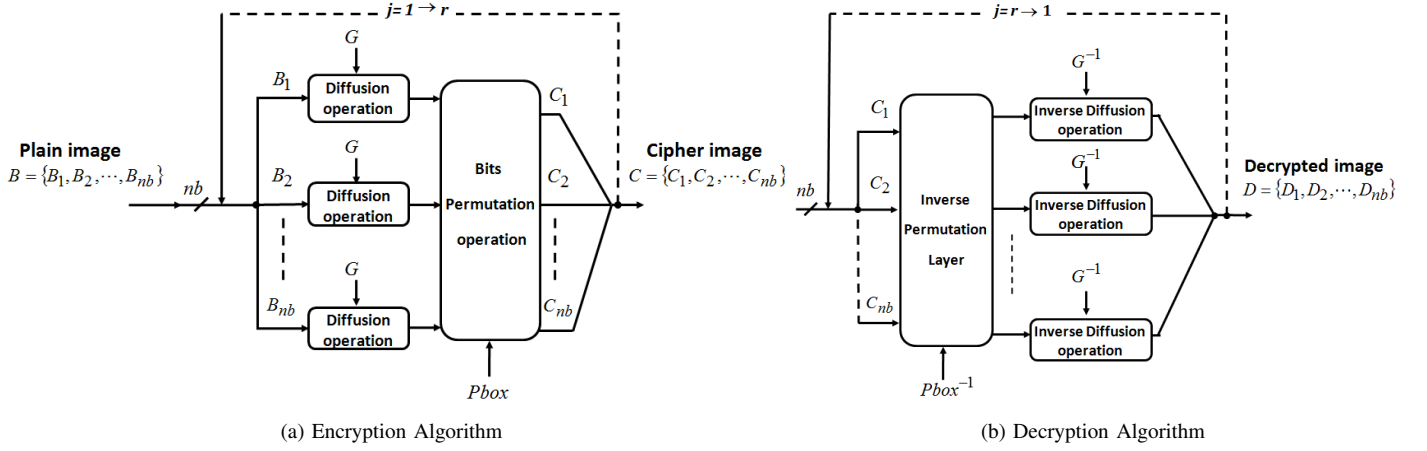


Figure 1: Architecture of the encryption(a) and decryption (b) algorithm described [1].

small image size 16×16 . Moreover, authors of [1] generalized the result to one round for the different sizes of any image, which is not logic. Therefore, the avalanche effect test (see the next subsection by applying the sensitivity test) was applied on the described scheme and a different result was found that is shown clearly in Table I for different sizes of images. It is clear, in this table, that 6 iterations are needed to reach an avalanche effect near 50%.

B. Sensitivity

The sensitivity refers to a huge change in the cipher text in response to a slight change in the original message itself. A cipher algorithm $E_K()$ is considered to be robust against chosen/known plain-text attacks, if it ensures the avalanche effect. In other words, the percentage of the Hamming distance (in bits) between the corresponding cipher image $C = E_k(I)$ and $C' = E_K(I')$ should be close to 50%, while I and I' only differ by one bit. An image I has been chosen that have all values equal to zero. I' is different from I by only one random pixel that has value equals to one. The sensitivity of the plain image PS is analyzed for 1000 random plain images and keys using the percentage of the Hamming distance, which is calculated as follows:

$$PS_w = \frac{\sum (Byte2bit(C_w) \oplus Byte2bit(C'_w))}{T} \times 100\%$$

$$= \frac{\sum Byte2bit(E_{K_w}(I)) \oplus Byte2bit(E_{K_w}(I'))}{T} \times 100\%$$

where T is the length in bits of the original and cipher images, C_w and C'_w are the corresponding w^{th} cipher images using I_w and I'_w and (K_w) secret keys respectively. All the elements of I'_w are equal to those of I_w , except a random Least Significant Bit (LSB) of a random byte, which was flipped and $w = 1, 2, \dots, 1000$.

According to the obtained results, the sufficient number of rounds, r should be ≥ 6 to be dependent on the size of

images as shown in Table I and Figure 2, where the size of images is square ($M \times M$). Therefore, to reduce the execution time with a good avalanche degree, r must be set to 6 for $M < 196$ and $r > 6$ for $M \geq 196$. Finally, r equals to 6 is sufficient to reach the avalanche effect for the different analyzed sizes of images (the maximum size of simulation that was analyzed was 512×512). Moreover, the obtained results illustrated here are reasonable, since increasing the image size will definitely increase the number of blocks, which requires a sufficient number of rounds to propagate the difference among blocks to reach the avalanche effect. Based on that, r cannot be set to 1 as indicated in [1]. Therefore, a lower degree of avalanche effect is reached, which means that it cannot immune the system against chosen/known plain-text attacks according to their configuration ($r = rp = 1$). Therefore, this cipher is insecure with this number of rounds. Consequently, after these results, r must be 6 to obtain the required level of security. On the other hand, this will lead to an increase in the execution time.

Figure 2(a) shows the average values of the percentage of the Hamming distance over 1000 random dynamic keys versus the number of rounds r . The obtained results show that the optimal number of iterations to reach the avalanche effect is 6 for the different sizes of images. Additionally, to ensure the independence between the plain and cipher images, (1) the percentage of the Hamming distance between I and its corresponding encrypted one C are computed as described above (see Eq. 2). The obtained results in Figure 2-(b) show that the independence between the plain and cipher images requires the same number of iterations of the avalanche effect. This means that to reach the independence and the avalanche effect, r should be ≥ 6 .

C. Analysis of the uniformity

To resist the common statistical attacks, the encrypted image should possess certain random properties. The most important one is that the frequency of each symbol of the encrypted

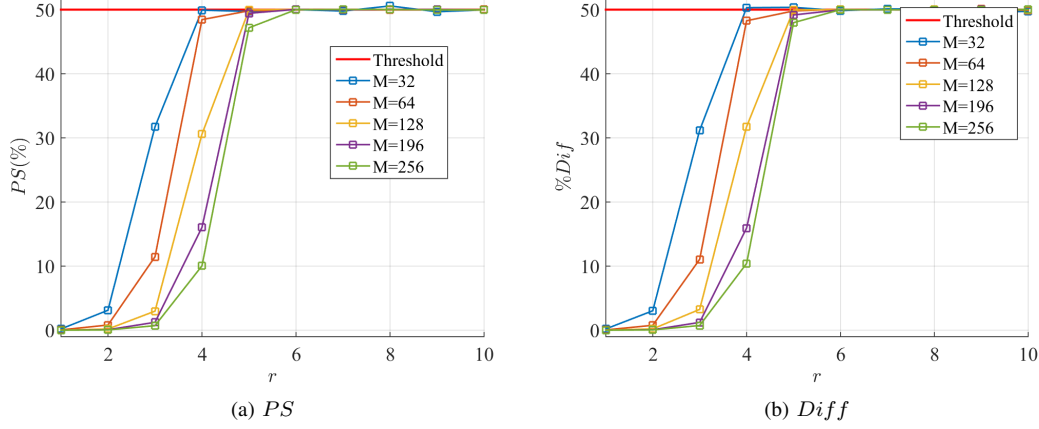


Figure 2: Variation of the average of the percent of the avalanche effect and the mean difference between plain and cipher-text over 1000 random keys versus the number of rounds r respectively.

Table I: Variation of the avalanche effect versus the size of image and the number of rounds r .

| $M \backslash r$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|------------------|--------|--------|--------|-------|--------|--------------|-------|
| 16×16 | 0.3092 | 4.2415 | 29.052 | 45.09 | 49.39 | 50.03 | 49.97 |
| 32×32 | 0.077 | 1.135 | 11.54 | 40.26 | 48.29 | 49.6 | 49.86 |
| 64×64 | 0.0193 | 0.342 | 5.720 | 44.70 | 49.99 | 50.08 | 49.64 |
| 128×128 | 0.004 | 0.082 | 1.407 | 15.00 | 47.34 | 50.03 | 49.9 |
| 196×196 | 0.0021 | 0.035 | 0.52 | 4.51 | 39.80 | 49.95 | 49.99 |
| 256×256 | 0.0012 | 0.0212 | 0.3366 | 5.348 | 42.441 | 50.01 | 49.97 |
| 300×300 | 0.0009 | 0.0152 | 0.2588 | 4.290 | 38.273 | 50.04 | 50.12 |
| 512×512 | 0.0003 | 0.005 | 0.087 | 1.429 | 19.688 | 49.99 | 50.02 |

image should be uniform. This means that each symbol has an occurrence probability close to $\frac{1}{n}$, where n is the number of symbols. In order to compute the level of uniformity of each encrypted image, the **Chi-square test** is applied as expressed in Equation 2:

$$\chi^2 = \sum_{i=0}^{Q-1} \frac{(o_i - e)^2}{e} \quad (2)$$

Where Q is the number of gray levels (here we work with gray scale images, $Q=256$), and o_i is the observed occurrence frequencies of each gray level (0-255) and e is the desired uniform frequency that equals to $\frac{len}{Q}$, where len is the length of image in byte level. This statistical test is used to compare the observed data with a specific hypothesis. Hence, the null hypothesis is formulated, which is then rejected or retained with the help of some statistical tests. The probability value below, which is the null hypothesis, is rejected and is called the alpha level or simply the "significant level". It is conventional to conclude that the null hypothesis is false if the probability value is less than 0.05 [26]. The level of significance of 0.05 (or 5%) is often chosen. In fact, with a significance level of 0.05, researchers can be 95 % confident that the results represent a non-chance finding [27]. Indeed, with a significant level of 0.05 and a number of intervals equal to 256, the chi-square reaches a maximal value equals to 293 [28]. So, all values lower than this value are acceptable and indicate the uniformity distribution of the histogram.

This criterion is verified by testing the chi-square for the previous mentioned images I under 1000 different dynamic keys. Figure 3 shows that the mean chi-square values become ≤ 293 after 6 iterations for all the dimension. This confirms the previous result and clearly indicates that $r \geq 6$ is sufficient to reach the independence avalanche effect, and uniformity property of the encrypted image under the proposed algorithm.

However, ensuring the security by reaching the avalanche effect introduces a hard challenge that is described in the following. This will have a high impact of a single bit change in the encrypted image and consequently a hard visual degradation is obtained and these results are described in the next section. This indicates clearly that a trade-off between the avalanche effect and error propagation is reached with this kind of scheme.

IV. PROPAGATION OF ERRORS

Indeed, an important criterion that should be ensured for any cipher is the tolerance error, which means that the error is not propagated. Interference and noise existing in the transmission channel are the main causes of error. However, a bit error means that a substitution of '0' bit into '1' bit or vice versa will take place. This error may propagate and leads to the destruction of data, which is a big challenge since a trade-off between the Avalanche effect and an error propagation is shown in [29]. In [1], if a bit error takes place in any

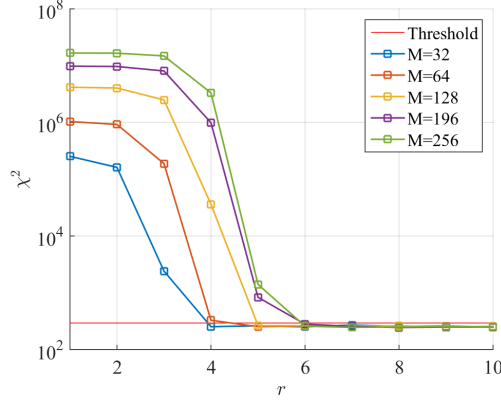


Figure 3: Variation of the average of the chi-square test over 1000 random keys versus the number of rounds r respectively, with $Tb = 256$.

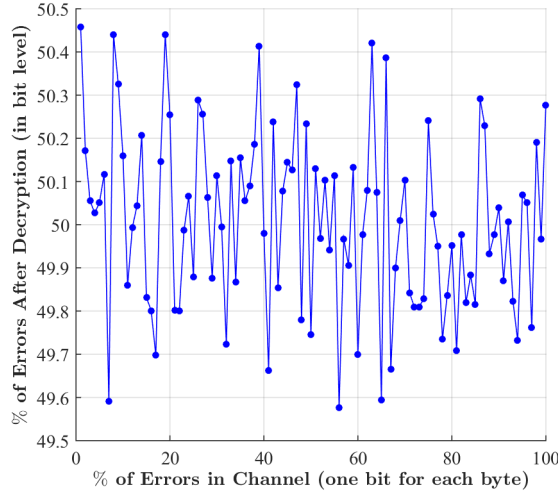


Figure 4: Variation of the impact of the error propagation according to the percentage of errors.

encrypted block, it will affect the overall decrypted image and the difference between both decrypted images are calculated according to Equation 2. The result is presented in Figure 4 which shows that the error is always close to 50%. As a result, we can deduce that the proposed approach is inefficient to overcome the propagation error. Therefore, any error in one byte will propagate to all other bytes which makes the system powerless against noisy and fading channels.

A. Visual Degradation

This test is specific for image and video contents and enables to quantify the visual degradation that it reaches by employing the cipher scheme with the effect of error propagation. In fact, the degradation operated on the decrypted image after any single change of any bit prevents the contents of an image from being recognized. To measure the visual degradation, two well known parameters are studied to measure the encryption visual quality which are Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM).

PSNR is derived from the Mean Squared Error (MSE), while MSE represents the cumulative squared error between an original and an encrypted image. A lower PSNR value indicates that there is a high difference between the original and the cipher images.

In addition, another metric is used and called Structural Similarity (SSIM) index [16], which is defined after the Human Visual System (HVS) and quantifies the similarity between two images. SSIM is in the interval $[0,1]$. A value of 0 means that there is no correlation between the original and the cipher images, while a value close to 1 means that both images are approximately the same. In this context, *PSNR* and *SSIM* are measured between two decrypted Lena images (where the second decrypted image corresponds to the encrypted image with a percent of error). Indeed, in Figure 5-(a) and (b), *PSNR* and *SSIM* are shown respectively. As shown, the variation of *PSNR* and *SSIM* versus the percentage of errors is presented. This low value validates that the proposed cipher provides a high difference between both decrypted images from the

lower error percentage. This means that a high and hard visual distortion is obtained from a small error percentage. Therefore, the cipher algorithm cannot be employed in practical systems that suffer from the error channel.

Moreover, in Table II the results are clearly showing the values of PSNR, SSIM and *Dif*. *Dif* is the sensitivity test that measures the difference between two decrypted images with a percentage of errors introduced in the encrypted image (we suppose that it is the effect of a channel noise in the encrypted image). It is close to 50%, which is relatively a high value that will prevent the recovery of the original image. As a conclusion, the proposed scheme suffers from the hard visual degradation caused by the channel error. This means that no useful visual information or structure about the original image could be revealed from the decrypted image if any error in the channel is introduced.

V. PERFORMANCE ANALYSIS

In practice, it is very important that the cipher requires less latency, memory and lower resources for the ciphering/deciphering process in order to be considered efficient. The presented encryption scheme employs bit permutation on the overall image, which requires a huge memory size and prevents its employment in tiny devices. The proposed scheme must undertake a higher number of rounds ($r = 6$) and consequently requires 5 times overhead in addition to the one presented in [1]. Thus, this proposal is not efficient in tiny devices which are battery limited and cannot respond to the needs of real time applications. In addition, the required size of memory and the execution time should always be at a minimum to reach a good encryption candidate.

A. Discussion and Cryptanalysis: Resistance against the well-known types of attacks

In the following, the typical cryptanalytic cases appearing in the literature are considered and a brief analysis of the proposed cipher against several cryptanalytic attacks is provided. The proposed cipher algorithm is considered to be public and the cryptanalyst has a complete knowledge about the employed confusion and diffusion primitives to know the technique used to build them but no knowledge about the secret key is available. The previous scheme of [1] can be broken by employing different types of attacks. It is not sufficient to achieve the required level of security since the scheme fails to resist statistical attacks (uniformity is not attained) in addition to chosen/known plain-text attacks. Therefore, differential attacks are based on studying the relation between two encrypted images resulting from a slight change, usually one bit difference compared to the original one. A successful sensitivity test shows how much a slight change in the plain-image or in the key will affect the resulted cipher image. Moreover, the key space used is fixed and can be $2^{4 \times q}$, which is not sufficient to prevent the brute-force attack. Finally, the problem of single image failure and accidental key disclosure is not taken into consideration by this scheme. Furthermore, differential and linear attacks would become

effective. Therefore, this cipher cannot resist different kinds of attacks.

VI. CONCLUSION AND FUTURE WORK

In this paper, we analyzed the previous cipher presented in [1]. In fact, we proved that this scheme has different weaknesses such as the wrong avalanche effect reached in addition to a short size of permutation key. This leads to consider the system insecure against different kinds of attacks. More important, error propagation was studied and its results were devastating on the decryption side since no useful data can be obtained when any bit is subjected to a channel noise. Therefore, this solution is not efficient since it requires a huge memory size, **higher** latency and cannot resist the channel error. In addition, it is not secure since it cannot face powerful attacks. These results are presented in order to prove the non credibility and the unsafe employment of [1]. For future works, we aim to build an efficient and secure lightweight image encryption scheme that will overcome all the stated challenges details in this paper.

REFERENCES

- [1] S. El Assad and M. Farajallah, "A new chaos-based image encryption system," *Signal Processing: Image Communication*, vol. 41, pp. 144–157, 2016.
- [2] E. Biham and A. Shamir, *Differential cryptanalysis of the data encryption standard*. Springer-Verlag New York, 1993, vol. 28.
- [3] J. Daemen and V. Rijmen, *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media, 2002.
- [4] N. A. Flayh, R. Parveen, and S. I. Ahson, "Wavelet based partial image encryption," in *Multimedia, Signal Processing and Communication Technologies, 2009. IMPACT'09. International*. IEEE, 2009, pp. 32–35.
- [5] T. Dan and W. Xiaojing, "Image encryption based on bivariate polynomials," in *Computer Science and Software Engineering, 2008 International Conference on*, vol. 6. IEEE, 2008, pp. 193–196.
- [6] S. M. Seyedzadeh and S. Mirzakuchaki, "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map," *Signal Processing*, vol. 92, no. 5, pp. 1202–1215, 2012.
- [7] X. Tong, M. Cui, and Z. Wang, "A new feedback image encryption scheme based on perturbation with dynamical compound chaotic sequence cipher generator," *Optics Communications*, vol. 282, no. 14, pp. 2722–2728, 2009.
- [8] A. Akhshani, S. Behnia, A. Akhavan, H. A. Hassan, and Z. Hassan, "A novel scheme for image encryption based on 2d piecewise chaotic maps," *Optics Communications*, vol. 283, no. 17, pp. 3259–3266, 2010.
- [9] S. M. Seyedzadeh, S. Mirzakuchaki, and R. E. Atani, "A novel image encryption algorithm based on hash function," in *Machine Vision and Image Processing (MVIP), 2010 6th Iranian*. IEEE, 2010, pp. 1–6.
- [10] A. Kumar and M. Ghose, "Extended substitution–diffusion based image cipher using chaotic standard map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, no. 1, pp. 372–382, 2011.
- [11] Z.-l. Zhu, W. Zhang, K.-w. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Information Sciences*, vol. 181, no. 6, pp. 1171–1186, 2011.
- [12] C. Huang, C.-W. Liao, S. Hsu, and Y. Jeng, "Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system," *Telecommunication Systems*, vol. 52, no. 2, pp. 563–571, 2013.
- [13] S. E. Borujeni and M. Eshghi, "Chaotic image encryption system using phase-magnitude transformation and pixel substitution," *Telecommunication Systems*, vol. 52, no. 2, pp. 525–537, 2013.
- [14] C. Li, M. Z. Chen, and K.-T. Lo, "Breaking an image encryption algorithm based on chaos," *International Journal of Bifurcation and Chaos*, vol. 21, no. 07, pp. 2067–2076, 2011.
- [15] R. Rhouma, E. Solak, and S. Belghith, "Cryptanalysis of a new substitution–diffusion based image cipher," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 7, pp. 1887–1892, 2010.

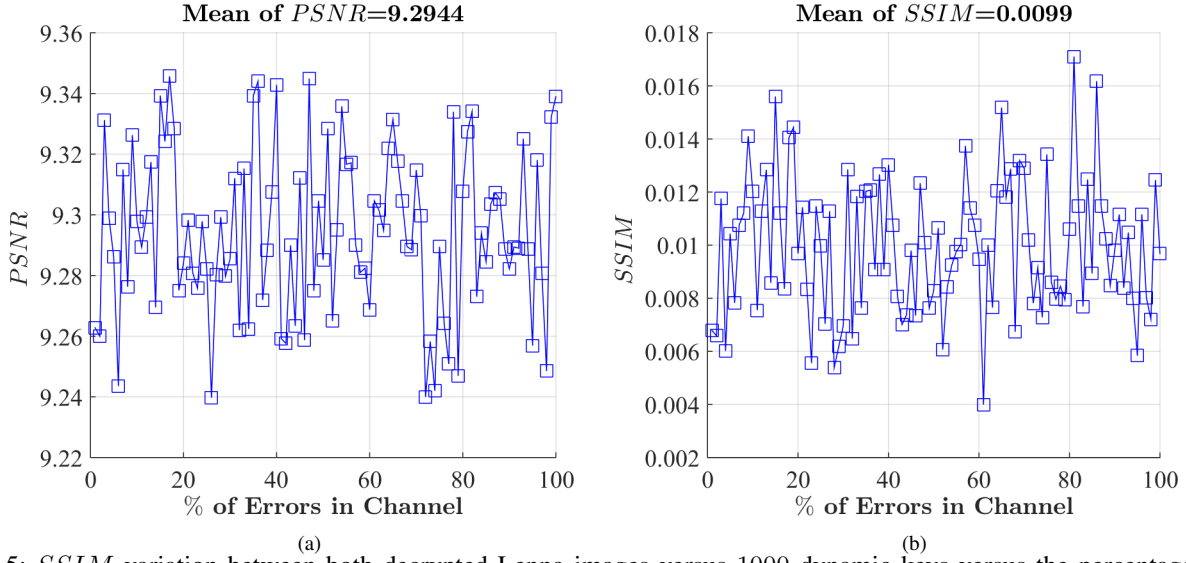


Figure 5: *SSIM* variation between both decrypted Lenna images versus 1000 dynamic keys versus the percentage of errors in channel.

Table II: Statistical results of sensitivity for Lenna image for 1000 random keys.

| Integer Diffusion matrices | | | | |
|----------------------------|---------|---------|---------|--------|
| | Min | Mean | Max | Std |
| <i>Dif</i> | 49.7505 | 50.0091 | 50.2399 | 0.1014 |
| PSNR | 9.2397 | 9.2944 | 9.3457 | 0.0275 |
| SSIM | 0.0040 | 0.0099 | 0.0171 | 0.0026 |

- [16] S. Li and X. Zheng, "Cryptanalysis of a chaotic image encryption method," in *Circuits and Systems, 2002. ISCAS 2002. IEEE International Symposium on*, vol. 2. IEEE, 2002, pp. II–708.
- [17] F. Huang and Y. Feng, "Security analysis of image encryption based on twodimensional chaotic maps and improved algorithm," *Frontiers of Electrical and Electronic Engineering in China*, vol. 4, no. 1, pp. 5–9, 2009.
- [18] D. Arroyo, C. Li, S. Li, G. Alvarez, and W. A. Halang, "Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm," *Chaos, Solitons & Fractals*, vol. 41, no. 5, pp. 2613–2616, 2009.
- [19] G. Alvarez and S. Li, "Cryptanalyzing a nonlinear chaotic algorithm (nca) for image encryption," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 11, pp. 3743–3749, 2009.
- [20] Q. Huynh-Thu and M. Ghanbari, "Scope of validity of psnr in image/video quality assessment," *Electronics letters*, vol. 44, no. 13, pp. 800–801, 2008.
- [21] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *Image Processing, IEEE Transactions on*, vol. 13, no. 4, pp. 600–612, 2004.
- [22] C. Paar and J. Pelzl, *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009.
- [23] Y. Wang, K.-W. Wong, X. Liao, T. Xiang, and G. Chen, "A chaos-based image encryption algorithm with variable control parameters," *Chaos, Solitons & Fractals*, vol. 41, no. 4, pp. 1773–1783, 2009.
- [24] H. Noura, "Design and simulation of efficient chaos based generators, crypto-systems and hash functions," Theses, UNIVERSITE DE NANTES, Aug. 2012. [Online]. Available: <https://hal.archives-ouvertes.fr/tel-01104996>
- [25] K. M. Alajel, W. Xiang, and J. Leis, "Error resilience performance evaluation of h. 264 i-frame and jowl for wireless image transmission," in *Signal Processing and Communication Systems (ICSPCS), 2010 4th International Conference on*. IEEE, 2010, pp. 1–7.
- [26] J.-B. du Prel, G. Hommel, B. Röhrig, and M. Blettner, "Confidence interval or p-value?: part 4 of a series on evaluation of scientific publications," *Deutsches Ärzteblatt International*, vol. 106, no. 19, pp. 335–9, 2009.
- [27] C. R. W. VanVoorhis and B. L. Morgan, "Understanding power and rules of thumb for determining sample sizes," *Tutorials in Quantitative Methods for Psychology*, vol. 3, no. 2, pp. 43–50, 2007.
- [28] J.-x. Chen, Z.-l. Zhu, C. Fu, L.-b. Zhang, and Y. Zhang, "An efficient image encryption scheme using lookup table-based confusion and diffusion," *Nonlinear Dynamics*, pp. 1–16, 2015.
- [29] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, and J.-J. Quisquater, "Overview on selective encryption of image and video: challenges and perspectives," *EURASIP Journal on Information Security*, vol. 2008, p. 5, 2008.